

**REMARKS**

In the above-identified Office Action, the Examiner indicated that the replacement ABSTRACT provided on 2/14/2006 was not legible and thus objected to the ABSTRACT. Further, the Examiner withdrew the indicated allowability of Claims 3, 8, 13 and 18, which were written in their independent form as Claims 1, 6, 11 and 16 and issued a rejection to Claims 1, 4 – 6, 9 – 11, 14 – 16, 19 and 20 under 35 U.S.C. §103(a) as being unpatentable over Alkhatib in view of Malagrino et al.

In response to the objection to the ABSTRACT, a new ABSTRACT is provided. Further, Applicants amended the SPECIFICATION to correct a minor typographical/grammatical error. In addition, Applicants amended the independent claims (i.e., Claims 1, 6, 11 and 16) to better claim the invention. No new matter is added to the Application since support for the addition to the claims can be found on page 12, lines 19 – 29.

By this amendment, Claims 1, 4 – 6, 9 – 11, 14 – 16, 19 and 20 remain pending in the Application. For the reasons stated more fully below, Applicants submit that the claims are allowable over the applied references. Hence, reconsideration, allowance and passage to issue are respectfully requested.

As mentioned in the Response to the First Office Action as well as disclosed in the SPECIFICATION, data is generally transmitted on a TCP/IP network in packets. Before being transmitted, therefore, several headers may be added to the packets. One of the headers that may be added is the Internet protocol (IP) header. The IP header has a two-byte identification field that is used to facilitate packet fragmentations. For example, as a packet is traversing the network, routers may fragment the packet into smaller packets. To ascertain that a receiving computer system is able to reconstruct a packet after it has been fragmented in transit, a transmitting computer system will give the packet an identity by entering a number into the IP identification field. If fragmented, each fragment will retain the IP identification number in its IP header. When the

AUS920010896US1

receiving computer system receives the fragments, using the IP identification number along with other fields in the IP header, it will be able to reconstruct the packet.

The two-byte identification field allows for 65,536 unique IP packets to be generated before the IP identification numbers recycle. With the use of a Gigabit Ethernet, however, this number of packets can be generated within one (1) second. Presently, it is rather common to have fragment re-assembly timers of thirty (30) seconds. Thus, using a fragment re-assembly timer of thirty (30) seconds with the Gigabit Ethernet may result in two or more different IP packets having the same IP identification number on the network. Hence, fragments from the two or more different packets may be mixed together. Consequently, a method of ascertaining that unique IP identification numbers are used on a Gigabit Ethernet network without modifying the IP identification field of the IP headers is needed. The present invention provides such method.

In accordance with the teachings of the invention, when sending IP packets using a Gigabit Ethernet, it is first determined whether a packet is permitted to be fragmented. (Note that if the "do-not fragment" bit in the IP header is set, the packet cannot be fragmented.) If it is determined that packet can be fragmented, a unique identification number is used in the IP header of the packet. In this case a unique identification number is a number that will not be used in the IP header of any other packet of data within the particular time span. If, on the other hand, the packet can be fragmented, then a non-unique identification number is used in the IP header of the packet. A non-unique identification number is a number that is used in the IP header of all packets of data that are not permitted to be fragmented. Thus, this scheme frees up the rest of the IP identification numbers for packets that may be fragmented.

The invention is set forth in claims of varying scopes of which Claim 1 is illustrative.

1. A method of maintaining a two-byte identification field of an Internet protocol (IP) header of a packet of data, the packet of data being transmitted over a network, the method comprising the steps of:

***determining whether the packet of data is permitted to be fragmented before being transmitted over the network wherein an identification number can be used more than once within a particular time span;***

***using a unique identification number in the IP header of the packet of data if the packet of data is permitted to be fragmented, the unique identification number being a number that will not be used in the IP header of any other packet of data within the particular time span; and***

***using a non-unique identification number in the IP header of the packet of data if the packet of data is not permitted to be fragmented, the non-unique identification number being a number that is used in the IP header of all packets of data that are not permitted to be fragmented to facilitate using unique identification numbers in the network.***  
(Emphasis added.)

The Examiner rejected the claims under 35 U.S.C. §103(a) as being anticipated by Alkhatib in view of Malagrino et al. Applicants respectfully disagree.

Alkhatib purports to teach a domain name routing system. According to the teachings of Alkhatib, a stub network which is a network owned by an organization that it is connected to the Internet through one or more gateways is used. Rather than use an entire set of global addresses for a Class A, B or C network, each corporate entity or stub network can be assigned one or a small number of global addresses. Each of the hosts of a corporate entity can be assigned a local address. The same local addresses can be used by many different corporate entities. When a source entity sends data to a destination entity in a stub network with a local address, the data is sent to a global address for the destination's network. The global address is assigned to a Domain Name Router in communication with the destination's network. The Domain Name  
AUS920010896US1

Router serves as a gateway between the Internet and the stub network. The Domain Name Router routes IP traffic between nodes on the Internet (identified by their globally unique IP addresses) and nodes in its stub network. The source entity embeds the destination's domain name and its own domain name somewhere inside the data. The Domain Name Router receives the data, extracts the destination's domain name from the data, translates that domain name to a local address in its stub network and sends the data to the destination.

However, Alkhatib does not show, teach or suggest the steps of ***determining whether the packet of data is permitted to be fragmented before being transmitted over the network wherein an identification number can be used more than once within a particular time span; using a unique identification number in the IP header of the packet of data if the packet of data is permitted to be fragmented, the unique identification number being a number that will not be used in the IP header of any other packet of data within the particular time span; and using a non-unique identification number in the IP header of the packet of data if the packet of data is not permitted to be fragmented, the non-unique identification number being a number that is used in the IP header of all packets of data that are not permitted to be fragmented to facilitate using unique identification numbers in the network.***

Malagrino et al purport to teach a method of efficiently reassembling fragments received at an intermediate station in a computer network. According to the teachings of Malagrino et al., an IP reassembly engine is used. The main controller of the IP reassembly engine comprises, inter alia, a frame buffer controller that cooperates with queuing and dequeuing logic to store and retrieve fragments to/from queues of the frame buffer. An input queue data structure is provided within the main controller for managing the queues of the frame buffer. The main controller is responsible for deciding whether a packet received by the IP reassembly engine is complete by checking status information maintained by a CAM (content addressable memory) subsystem. The main controller also

AUS920010896US1

manages the CAM by deleting packet entries and all related fragment entries that have expired. This latter task is performed in accordance with a timer handling process that periodically compares a current time with an expiration time stored in an expiration time field of each CAM entry.

However, just as I the case of Alkhatib, Malagrino et al. do not show, teach or suggest the steps of ***determining whether the packet of data is permitted to be fragmented before being transmitted over the network wherein an identification number can be used more than once within a particular time span; using a unique identification number in the IP header of the packet of data if the packet of data is permitted to be fragmented, the unique identification number being a number that will not be used in the IP header of any other packet of data within the particular time span; and using a non-unique identification number in the IP header of the packet of data if the packet of data is not permitted to be fragmented, the non-unique identification number being a number that is used in the IP header of all packets of data that are not permitted to be fragmented to facilitate using unique identification numbers in the network.***

Consequently, combining the teachings of Alkhatib with those of Malagrino et al. does not teach the claimed invention. Therefore, Applicants submit that Claim 1, as well as its dependent claims should be allowable. The other independent claims (i.e., Claims 6, 11 and 16), which all incorporate the emboldened-italicized limitations in the above-reproduced Claim 1 and their dependent claims should be allowable as well. Hence, Applicants once more request reconsideration, allowance and passage to issue of the claims in the application.

Appl. No. 10/087,939  
Response dated 12/20/2006  
Reply to Office Action of 09/25/2005

Respectfully Submitted

By: 

Volel Emile  
Attorney for Applicants  
Registration No. 39,969  
(512) 306-7969

AUS920010896US1